REMARKS

The Examiner has objected to the drawings. Such objections have been avoided by virtue of the clarifications made hereinabove to the drawings.

The Examiner has rejected Claims 12-22, and 26 under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Such rejection is deemed moot in view of the clarifications made hereinabove to such claims.

The Examiner has further rejected Claims 1-3, 5-7, 9-10, 12-14, 16-18, 20-21, and 23-27 under 35 U.S.C. 102(e) as being anticipated by Shostack et al. (U.S. Patent No.: 6,298,445). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove. Specifically, applicant has amended each of the independent claims to include the subject matter of former dependent Claims 2-3 and 7-8 et al.

In the Examiner's action, the Examiner relies on the following excerpt from Shostack to meet applicant's claimed "receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network," and "performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer."

> "The push system integrates the software enhancement into existing programs. Additionally, the integration can also perform a check on the integrity and authenticity of the software enhancement provided. This feature determines whether the user being sent the software enhancement is eligible, and checks the integrity and authenticity of the software enhancement. In determining the integrity and authenticity of the software enhancement, the push system can use digital signatures or other cryptographic techniques. In the disclosed embodiment, digital signatures are used to encode the software enhancement by using a signing key, and an authorized local user 6 or customer possesses the correct key for validating the original message." (see col. 8, lines 19-31)
>
> "A fourth module accesses the database and assesses security vulnerabilities of a remote computer connected to the network. A fifth module receives an update to the database and updates the database. A

sixth module is a communications module that allows communication between the integrated system and a similar system." (see col. 3, lines 15-20)

Applicant respectfully disagrees this assertion. In particular, Shostack merely discloses encryption in the context of updating, not "commands for executing a risk-assessment scan from a remote computer utilizing a network." Moreover, Shostack merely makes a blanket suggestion that the system may "assess the security vulnerabilities of a remote computer connected to the network." This, in no way, rises to the level of specificity of applicant's claimed assessment of vulnerabilities on a first computer with an agent installed thereon, where such agent (and the associated risk-assessment scanner) is controlled by encrypted commands from a second computer, as claimed.

Instead, Shostack merely suggests "allow[ing] a remote computer to first connect to a network service then accepts information from the service and ... also interrogates the service." This simply falls short of applicant's claim limitations.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Shostack reference, for the reasons noted above. Nevertheless, despite the foregoing paramount differences and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to include the following subject matter of former dependent Claims 2-3 and 7-.8 et al:

"wherein the agent includes a plurality of risk-assessment modules;

wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer;

wherein the commands each indicate at least one of the risk-assessment modules;

wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters."

With respect to the subject matter of Claim 3 et al. (now incorporated into each of the independent claims), the Examiner relies on the following excerpt from Shostack to meet applicant's claimed "wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer."

> "A fourth module accesses the database and assesses security vulnerabilities of a remote computer connected to the network." (see col. 12, lines 7-9)

Again, Shostack merely makes a blanket suggestion that the system may "assess the security vulnerabilities of a remote computer connected to the network." Further, Shostack merely elaborates by stating that "allow[ing] a remote computer to first connect to a network service then accepts information from the service and ... also interrogates the service." This simply falls short of applicant's assessment of vulnerabilities on a first computer with an agent installed thereon, where such agent (and the associated risk-assessment scanner) is controlled by encrypted commands from a second computer, as claimed.

With respect to the subject matter of Claim 8 et al. (now incorporated into each of the independent claims), the Examiner has rejected such claim, along with Claims 4, 15, and 19 under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. Patent No.: 6,298,445), in view of Orchier (U.S. Patent No.: 6,070.244). Applicant respectfully disagrees with such rejection.

Specifically, the Examiner relies on the following excerpt from Orchier to meet applicant's claimed "wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters."

> "The manual maintenance agent 86 takes inputs from the user and converts them into platform independent security maintenance

> instructions which are then processed by the maintenance agent abstraction facility 90. Examples of platform independent security maintenance categories and data are as follows:
>
> AddUserAccount(id, platformList, name, Payroll Number, expenseCode)
>
> RemoveUserAccount(id, platformList)
>
> AddUserAccountToGroup(id, platformList, GroupName)
>
> RemoveUserAccountFromGroup(id, platformList, GroupName)
>
> ModifyUserAccountName(id, platformList, name)
>
> ModifyUserAccountPay(id, platformList, Pay)
>
> ModifyUserAccountExpenseCode(id, platformList, expenseCode)
>
> DisableUserAccount(id, platformList)
>
> FIG. 8c shows the screen used to designate how often data should be collected. FIG. 8d shows the screen used to designate the server from which data should be collected. FIG. 8e shows the screen used to designate high risk applications. FIG. 8f shows the screen used to designate the environment. FIG. 8g shows the screen used to designate high risk reports. FIG. 8h shows the screen used to designate event code mapping of native codes to the common system code." (see col. 14, lines 25-52)

Orchier, however, merely makes a general statement regarding security maintenance. Such general teaching, however, simply does not rise to the level of specificity of applicant's claimed "risk-assessment modules," let alone commands that are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

With respect to the dependent claims, applicant has carefully reviewed the excerpts relied upon by the Examiner to reject the same, and has found serious deficiencies in the Examiner's application of the prior art. Just by way of example, the Examiner relies on the following excerpt from Orchier to meet applicant's claimed "wherein the risk-assessment modules are selected for the agent based on specifications of the local computer" (see Claim 4 et al.).

> "The invention uses a layered software architecture, enabling a separation of basic functions from the complications of differing technologies, and facilitating automated handling of many operations. The architecture can be viewed at a very high level as consisting of two layers: technology specific and technology independent. The technology specific layer consists of many groups of software modules, each group addressing the complexities of a single technology (e.g., NetWare.TM. 3.1, Windows NT, AIX, Sybase, etc.). The primary functions of the technology specific layer are extracting and maintaining security data on the target platforms, and converting the data to and from the common data model used by the technology independent layer." (see col. 2, lines 15-28)

After carefully reviewing such excerpt and the remaining Orchier reference, however, it is clear that Orchier merely suggests technology specific layers for security maintenance. This simply fails to rise to the level of specificity of applicant's claimed selection of risk-assessment modules based on specifications of the local computer, as claimed.

Still yet, the Examiner relies on col. 3, lines 6-37; col. 7, lines 20-30; col. 12, lines 27-40; and col. 13, lines 18-30 from Shostack to meet applicant's claimed "wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command" (see Claim 5 et al.).

Applicant respectfully disagrees with this assertion. Orchier merely suggests general vulnerability testing, and lacks at least the following emphasized features of the foregoing claimed subject matter, especially when taken in combination: "wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command" (emphasis added).

Even still, the Examiner relies on the following excerpt from Shostack to meet applicant's claimed "transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network" (see Claim 9 et al.), and "receiving feedback to the results from the remote computer utilizing the network" (see Claim 10 et al.).

> "transmitting reports or data for purposes of analysis, reporting to a management station ...
>
> The GUI 70 may also provide a reporting mechanism. The GUI 70 may also include several means for reporting various network transactions. In the disclosed invention, the GUI 70 includes a log view 80 may allow a user to view a text version the update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log." (see col. 13, lines 24-25 and lines 37-44)

After carefully reviewing such excerpts and the remaining Shostack reference, however, it is clear that Shostack merely suggests reporting and a GUI for facilitating the same. This, at best, may be considered a one-way communication similar (but not identical) to the subject matter of Claim 9, but clearly fails to satisfy the claimed two-way communication, namely involving applicant's feedback to the results received from the remote computer utilizing the network, as claimed

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the following additional dependent claims that have been added for full consideration:

"wherein the feedback is active" (see Claim 28);

"wherein the feedback includes additional commands and additional modules for correcting the vulnerabilities in response to the additional commands" (see Claim 29);

"wherein the feedback is passive" (see Claim 30);

"wherein the feedback includes descriptions as to how to correct the vulnerabilities" (see Claim 31);

"wherein the results include a log of the risk-assessment scan" (see Claim 32);

"wherein the results include an identification of the vulnerabilities" (see Claim 33);

"wherein a plurality of the commands are each associated with only one of the risk-assessment modules" (see Claim 34); and

"wherein a different set of risk-assessment modules exists on different local computers, based on a platform associated with each of the local computers" (see Claim 35).

Yet again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees

due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P011/01.116.01).

Respectfully submitted,

By: _____ Date: 12/22/04

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, PC
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573